IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

Appl. No.	: **09/896,197**
Applicant(s)	: **ROELSE, Petrus L.**
Filed	: **29 Jun 2001**
TC/A.U.	: **2136**
Examiner	: **SHIFERAW, Eleni A.**
Atty. Docket	: **NL-000365**

CERTIFICATE OF MAILING OR TRANSMISSION
I certify that this correspondence is being:
[ ] deposited with the U.S. Postal Service with sufficient postage as first-class mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
[X] transmitted by facsimile to the U.S. Patent and Trademark Office at **571-273-8300**.
On: 27 August 2005
By: [signature]

Title: **SUBSTITUTION-BOX FOR SYMMETRIC-KEY CIPHERS**

Mail Stop: **APPEAL BRIEF - PATENTS**
Commissioner for Patents
Alexandria, VA 22313-1450

APPEAL UNDER 37 CFR 41.37

Sir:

This is an appeal from the decision of the Examiner dated 5 April 2005, finally rejecting claims 1-20 of the subject application.

This paper includes (each beginning on a separate sheet):

1. **Appeal Brief, with appendices; and**
2. **Credit card authorization in the amount of $500.**

APPEAL BRIEF

I. REAL PARTY IN INTEREST

The above-identified application is assigned, in its entirety, to **Koninklijke Philips Electronics N. V.**

II. RELATED APPEALS AND INTERFERENCES

Appellant is not aware of any co-pending appeal or interference which will directly affect or be directly affected by or have any bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1 and 14 are canceled.

Claims 2-13 and 15-20 are pending in the application.

Claims 2-13 and 15-20 stand rejected by the Examiner under 35 U.S.C. 102(b).

These rejected claims are the subject of this appeal.

IV. STATUS OF AMENDMENTS

An amendment was filed on 21 May 2005, subsequent to the final rejection in the Office Action. This amendment was admitted, per the Advisory Action of 7 June 2005.

A supplemental amendment was filed on 23 August 2005, subsequent to the final rejection in the Office Action. This amendment canceled claim 14, rewrote claim 18 in independent form, and amended the dependent claims accordingly.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The invention relates to a cryptographic process that uses a non-linear operation in the form of a Substitution-box (S-box). The S-box applies a permutation to N input bits to produce M output bits, where, generally, M is less than N (Applicant's page 1, lines 10-13). As is known in the art, different permutations have different cryptographic strengths and weaknesses, such as inherent resistance to differential cryptoanalysis and resistance to linear cryptoanalysis (page 1, lines 18-20). In this invention, each S-box has access to two or more permutations (page 6, lines 4-6). As each input block is being processed, one of the permutations is dynamically selected for applying the non-linear operation in each S-box (page 1, line 28-29; also page 6, line 22).

In a preferred embodiment, each of the permutations available to the S-box compensates for weaknesses of the other permutation(s) (page 2, lines 6-8; also page 11, lines 8-14). For example, the differential characteristics of two permutations that compensate each other are illustrated at pages 9 and 10 of the applicant's specification. Note that for each occurrence of a "4" in the table of page 9, corresponding to a (maximum) probability of ¼ (4/16), a "0" appears in the table of page 10, corresponding to a (minimum) probability of 0 (0/16). Similarly, each "4" in the table of page 10 has a corresponding "0" in the table of page 9. A similar pair of tables, illustrating the linear characteristics of each permutation, is presented at pages 12 and 13.

As claimed in independent claim 2, upon which claims 3-12 depend, the invention comprises a method for cryptographically converting an input data block into an output data block that includes selecting a select permutation from a predetermined set of at least two permutations (page 6, lines 4-6), and performing a non-linear substitution operation on the input data block based on the select permutation (page 6, lines 20-22), wherein the set of permutations is formed such that a cryptographic weakness in one of the permutations of the set is at least

partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set (page 7, line 32 – page 8, line 13).

As claimed in dependent claim 3, the set of permutations are such that for each non-trivial differential characteristic having a maximum probability in any of the permutations, the differential characteristic has a lower probability in at least one of the other permutations of the set (page 7, lines 20-22).

As claimed in dependent claim 4, the differential characteristic has a probability equal to zero in at least one of the permutations (page 10, lines 4-6).

As claimed in dependent claim 5, the data block consists of 4 data bits, and the maximum probability equals ¼ (page 9, lines 12-14).

As claimed in dependent claim 6, the set of permutations are such that for each non-trivial linear characteristic with probability that equals a minimum or maximum probability in any of the permutations, this linear characteristic has a probability closer to ½ in at least one of the other permutations of the set (page 11, lines 5-7).

As claimed in dependent claim 7, the linear characteristic has a probability equal to ½ in at least one of the permutations (page 11, lines 8-10).

As claimed in dependent claim 8, the data block consists of 4 data bits, the minimum probability is ¼, and the maximum probability is ¾ (page 12, lines 7-9).

As claimed in dependent claim 10, selecting the select permutation is based on an encryption key (page 6, lines 17-19).

As claimed in dependent claim 11, selecting the permutation is performed under control of a bit of an encryption key (page 6, lines 17-19).

As claimed in independent claim 13, the invention comprises a system (FIGs. 2 and 3) for cryptographically converting an input data block into an output data block. The system includes an input for receiving the input data block (page 3, lines 6-7), a storage for storing a predetermined set of at least two permutations associated with an S-box (page 6, lines 4-6); a cryptographic processor for performing a non-linear operation on the input data block using an S-box based on a permutation (page 3, lines 7-8); the processor being operative to, each time before using the S-box, (pseudo-)randomly selecting the permutation from the stored set of permutations associated with the S-box (page 6, lines 4-6); and an output for outputting the processed input data block (page 3, lines 10-11).

As claimed in independent claim 18, upon which claims 15-17 and 19-20 depend, the invention comprises a cryptographic encoder that includes one or more encryption stages (FIGs. 1A, 1B). Each stage of the one or more encryption stages includes a non-linear substitution module (f in FIGs. 1A, 1B) that is configured to receive a control signal (K_i) and a set of data bits ($X_{i-1}(R)$). The non-linear substitution module includes a plurality of substitution boxes (220 in FIG. 3), and each of the substitution boxes is configured to receive at least a subset of the control signal ($k_0^{(i)}$) and a subset of the set of data bits (each of the four-bit inputs to the S-boxes 220). Each substitution box substitutes a first output value for the subset of the set of data bits if the subset of the control signal is a first value ($k_0^{(i)}$ = "0" row of table at lines 3-4 of page 8), and substitutes a second output value for the subset of the set of data bits if the subset of the control signal is a second value ($k_0^{(i)}$ = "1" row of table at lines 3-4 of page 8) (as detailed at page 8, lines 5-9). The second output value is formed such that a cryptographic weakness in the first output value is at least partially compensated by a corresponding cryptographic strength in the second output value (page 2, lines 6-8; also page 11, lines 8-14).

As claimed in dependent claim 19, for each non-trivial differential characteristic having a maximum probability in a set of 2^n elements that provide the first output value, this differential characteristic has a lower probability in the set of 2^n elements that provide the second data output value (page 8, lines 16-18).

As claimed in dependent claim 20, for each non-trivial linear characteristic that equals a minimum or maximum probability in a set of 2^n elements that provide the first output value, this linear characteristic has a probability closer to ½ in the set of 2^n elements that provide the second data output value (page 11, lines 5-7).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 2-13 and 15-20 stand rejected under 35 U.S.C. 102(b) over Heys et al. ("The Design of Secure Block Ciphers", May 1994, hereinafter Heys).

VII. ARGUMENT

Claims 2-13 and 15-20 stand rejected under 35 U.S.C. 102(b) over Heys

Claims 2-12

Independent claim 2, upon which claims 3-12 depend, claims a method for cryptographically converting an input data block into an output data block that includes selecting a select permutation from a predetermined set of at least two permutations, and performing a non-linear substitution operation on the input data block based on the select permutation, wherein the set of permutations is formed such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set.

Heys teaches methods for creating permutations for use in substitution boxes. Heys teaches criteria that should be used for selecting a permutation for embodiment into an S-box. Heys teaches that: "An S-box in the network is defined as an n-bit bijective mapping S" (page 2, left column, lines 2-3). The applicant notes Heys' use of the *singular* article "an" when referring to the mapping S. Heys does not disclose providing multiple mappings (predetermined permutations) in each S-box, and selecting one of the multiple mappings for performing a substitution operation on an input block.

The Office action asserts that because Heys teaches selecting a (single) permutation for embodiment in an S-box, this selection corresponds to the applicant's claimed selection of a select permutation from a predetermined set of at least two permutations.

Assuming in argument that this interpretation of Heys corresponds to the applicant's claimed selection, the applicant respectfully notes that the applicant's predetermined set of permutations is formed such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set. All of Heys' permutations/mappings satisfy the criteria set by Heys to provide "good diffusion and nonlinearity properties" (Abstract, lines 9-11), the details of which are given at section IV (S-box design). Heys does not distinguish between mappings within the set of mappings that satisfy the given criteria, and does not identify differing cryptographic strengths possessed by each mapping. Therefore, Heys cannot be said to form the set of permutations such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set, as specifically claimed by the applicant.

Because Heys does not teach selecting a permutation from a predetermined set of permutations that are formed such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set, as

specifically claimed in claim 1, the applicant respectfully maintains that the rejection of claims 1-12 under 35 U.S.C. 102(b) over Heys is unfounded. Therefore, the applicant requests that the rejection of claims 1-12 under 35 U.S.C. 102(b) over Heys be reversed by the Board and the claims be allowed to issue.

In the alternative, should the Board decide to sustain the rejection of claim 1, the following remarks are provided regarding select dependent claims.

Claim 3

Dependent claim 3 claims that the set of permutations are such that for each non-trivial differential characteristic having a maximum probability in any of the permutations, the differential characteristic has a lower probability in at least one of the other permutations of the set.

Heys does not address the specific differential characteristics of each permutation, and does not teach comparing the characteristics of each of the permutations in a predetermined set to each other. Thus, Heys cannot be said to include a permutation that includes a lower differential probability corresponding to each occurrence of a maximum probability in another permutation, as specifically claimed in claim 3.

Claim 4

Dependent claim 4 claims that the differential characteristic has a probability equal to zero in at least one of the permutations.

Heys does not address the specific differential characteristics of each permutation, and thus cannot be said to teach at least one permutation having a differential probability equal to zero, as specifically claimed in claim 4.

Claim 5

Dependent claim 5 claims a data block of 4 data bits, wherein the maximum probability equals ¼.

Heys does not address the specific differential characteristics of each permutation, and does not address a maximum probability associated with each permutation. Thus Heys cannot be said to teach a maximum probability of ¼, as specifically claimed in claim 5.

Claim 6

Dependent claim 6 claims that the set of permutations are such that for each non-trivial linear characteristic with probability that equals a minimum or maximum probability in any of the permutations, this linear characteristic has a probability closer to ½ in at least one of the other permutations of the set.

Heys does not address the specific characteristics of each permutation, does not address linear characteristics of the permutations, does not address minimum and maximum probabilities, and does not teach providing a linear characteristic having a probability closer to ½ in one of the permutations of the set for each linear characteristic in another permutation having a minimum or maximum probability, as specifically claimed in claim 6.

Claim 7

Dependent claim 7 claims that the linear characteristic has a probability equal to ½ in at least one of the permutations.

Heys does not address the specific characteristics of each permutation, does not address linear characteristics of the permutations, and does not teach a permutation having a probability equal to ½, as specifically claimed in claim 7.

Claim 8

Dependent claim 8 claims a 4-bit data block with linear characteristics having a minimum probability of ¼, and the maximum probability of ¾.

Heys does not address the specific characteristics of each permutation, does not address linear characteristics of the permutations, does not address minimum and maximum probabilities, and does not teach a 4-bit data block with linear characteristics having a minimum probability of ¼, and the maximum probability of ¾, as specifically claimed in claim 8.

Claims 10 and 11

Dependent claim 10 claims selecting the select permutation based on an encryption key. Dependent claim 11 claims that a bit of the encryption key controls the selection of the permutation.

Heys teaches a method for selecting a permutation for embodiment into an S-box. This selection is performed independent of the particular key that is used to encode or decode data using the S-box. Although the key affects the resultant output of the permutation, the key does not affect the selection of the permutation, as specifically claimed in claims 10 and 11.

Claim 13

Independent claim 13 claims a system for cryptographically converting an input data block into an output data block that includes a processor that (pseudo-)randomly selects a permutation from a stored set of permutations associated with an S-box each time before using the S-box to perform a nonlinear operation on the input data.

Heys teaches a cryptographic system (FIG. 1) and a technique for selecting a permutation for embodiment into each S-box. Heys specifically teaches: "An S-box in the network is defined as an n-bit bijective mapping S" (page 2, left column, lines 2-3). Heys does not teach a processor that randomly selects a permutation from a set of permutations each time before using the S-box.

Because Heys fails to teach a processor that randomly selects a permutation from a set of permutations each time before using the S-box to perform a nonlinear operation on the input data, as specifically claimed in claim 13, the applicant respectfully maintains that the rejection of claim 13 under 35 U.S.C. 102(b) over Heys is unfounded. Therefore, the applicant requests that the rejection of claim 13 under 35 U.S.C. 102(b) over Heys be reversed by the Board and the claim be allowed to issue.

Claims 15-20

Independent claim 18, upon which claims 15-17 and 19-20 depend, claims a cryptographic encoder that includes a plurality of substitution boxes, wherin each of the substitution boxes substitutes a first output value for the subset of the set of data bits if the subset of the control signal is a first value, and substitutes a second output value for the subset of the set of data bits if the subset of the control signal is a second value, and the second output value is formed such that a cryptographic weakness in the first output value is at least partially compensated by a corresponding cryptographic strength in the second output value.

Heys teaches methods for creating permutations for use in substitution boxes. Heys does not address the specific characteristics of each permutation, and does not teach forming a set of permutations such that the cryptographic strength of one permutation compensates the cryptographic weakness in another permutation of the set. The weakness of a substitution is exhibited in its output. Heys does not address the specific characteristics of the output of each permutation, and cannot be said to teach forming a second output value such that a cryptographic weakness in a first output value is at least partially compensated by a corresponding cryptographic strength in the second output value.

Because Heys does not teach a cryptographic encoder that forms a second output value of a substitution box such that a cryptographic weakness in a first output value of the substitution box is at least partially compensated by a corresponding cryptographic strength in the second output value, as specifically claimed in claim 18,

the applicant respectfully maintains that the rejection of claim 18 under 35 U.S.C. 102(b) over Heys is unfounded. Therefore, the applicant requests that the rejection of claims 15-20 under 35 U.S.C. 102(b) over Heys be reversed by the Board and the claim be allowed to issue.

In the alternative, should the Board decide to sustain the rejection of claim 18, the following remarks are provided regarding select dependent claims.

Claim 19

Dependent claim 19 claims that for each non-trivial differential characteristic having a maximum probability in a set of 2^n elements that provide the first output value, this differential characteristic has a lower probability in the set of 2^n elements that provide the second data output value.

Heys does not address the specific differential characteristics of each output of the S-boxes, and does not teach comparing the outputs to each other. Thus, Heys cannot be said to include an output that provides a lower differential probability corresponding to each occurrence of a maximum probability in another output, as specifically claimed in claim 19.

Claim 20

Claim 20 claims that for each non-trivial linear characteristic that equals a minimum or maximum probability in a set of 2^n elements that provide the first output value, this linear characteristic has a probability closer to ½ in the set of 2^n elements that provide the second data output value.

Heys does not address the specific characteristics of each output, does not address linear characteristics of the outputs, does not address minimum and maximum probabilities, and does not teach providing a linear characteristic having a probability closer to ½ in one of the outputs for each linear characteristic in another output having a minimum or maximum probability, as specifically claimed in claim 20.

CONCLUSIONS

Because Heys does not teach selecting an permutation from a predetermined set of permutations, wherein the predetermined set is formed such that the cryptographic strength of one permutation compensates for the cryptographic weakness of another permutation in the set, as specifically claimed in claim 1, the applicant respectfully requests that the Examiner's rejection of claims 1-12 under 35 U.S.C. 102(b) be reversed by the Board, and the claims be allowed to pass to issue.

Because Heys does not teach a processor that randomly selects a permutation from a set of permutations each time before using the S-box to perform a nonlinear operation on the input data, as specifically claimed in claim 13, the applicant respectfully requests that the Examiner's rejection of claim 13 under 35 U.S.C. 102(b) be reversed by the Board, and the claims be allowed to pass to issue.

Because Heys does not teach selecting between two outputs based on a key value, wherein the outputs are formed such that a cryptographic strength of one output compensates for the cryptographic weakness of the other output, as specifically claimed in claim 18, the applicant respectfully requests that the Examiner's rejection of claims 15-20 under 35 U.S.C. 102(b) be reversed by the Board, and the claims be allowed to pass to issue.

Respectfully submitted,

Robert M. McDermott, Attorney
Registration Number 41,508
804-493-0707

CLAIMS APPENDIX

1. (Cancelled).

2. A method for cryptographically converting an input data block into an output data block; the method including:

selecting a select permutation from a predetermined set of at least two permutations, and

performing a non-linear substitution operation on the input data block based on the select permutation,

wherein the set of permutations is formed such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set.

3. A method as claimed in claim 2, wherein

the data block consists of n data bits and

each permutation of the set of permutations is a set of 2^n elements, where each non-trivial differential characteristic of each permutation in this set has a probability that is less than or equal to a maximum probability;

the set of permutations being formed by permutations which have been selected such that for each non-trivial differential characteristic having the maximum probability in any of the permutations, this differential characteristic has a lower probability in at least one of the other permutations of the set.

4. A method as claimed in claim 3, wherein the differential characteristic has a probability equal to zero in at least one of the permutations.

5. A method as claimed in claim 4, wherein $n = 4$, and the maximum probability equals ¼.

6. A method as claimed in claim 2, wherein

the data block consists of *n* data bits and

each permutation of the set of permutations is a set of 2^n elements, where each non-trivial linear characteristic of each permutation in this set has a probability of at least a minimum probability and at most a maximum probability,

the set of permutations being formed by permutations which have been selected such that for each non-trivial linear characteristic with probability that equals the minimum or maximum probability in any of the permutations, this linear characteristic has a probability closer to ½ in at least one of the other permutations of the set.

7. A method as claimed in claim 6, wherein the linear characteristic has a probability equal to ½ in at least one of the permutations.

8. A method as claimed in claim 6, wherein $n = 4$, the minimum probability is ¼, and the maximum probability is ¾.

9. A method as claimed in claim 2, wherein the set of permutations consists of two permutations.

10. A method as claimed in claim 2, wherein

selecting the select permutation is based on an encryption key.

11. A method as claimed in claim 9, wherein

selecting the permutation is performed under control of a bit of an encryption key.

12. A computer program product where the program product is operative to cause a processor to perform the method of claim 2.

13. A system for cryptographically converting an input data block into an output data block; the system including:

- an input for receiving the input data block;
- a storage for storing a predetermined set of at least two permutations associated with an S-box;
- a cryptographic processor for performing a non-linear operation on the input data block using an S-box based on a permutation; the processor being operative to, each time before using the S-box, (pseudo-)randomly selecting the permutation from the stored set of permutations associated with the S-box; and
- an output for outputting the processed input data block.

14. (Canceled)

15. The cryptographic encoder of claim 18, wherein

each stage of the one or more encryption stages further includes

an addition module that is configured to combine at least a subset of a key with a data input to provide the set of data bits to the non-linear substitution module.

16. The cryptographic encoder of claim 15, wherein

the control signal includes another subset of the key.

17. The cryptographic encoder of claim 15, wherein

each stage of the one or more encryption stages further includes

a transformation module that is configured to transform the output values from the substitution boxes to provide therefrom an encrypted data output.

18. A cryptographic encoder comprising:

one or more encryption stages,

each stage of the one or more encryption stages including

a non-linear substitution module that is configured to receive a control signal and a set of data bits,

wherein

the non-linear substitution module includes a plurality of substitution boxes;

each of the substitution boxes is configured to receive at least a subset of the control signal and a subset of the set of data bits, and:

substitutes a first output value for the subset of the set of data bits if the subset of the control signal is a first value, and

substitutes a second output value for the subset of the set of data bits if the subset of the control signal is a second value, and

the second output value is formed such that a cryptographic weakness in the first value is at least partially compensated by a corresponding cryptographic strength in the second output value.

19. The cryptographic encoder of claim 18, wherein

the subset of the set of data bits consists of n data bits and

each of the first and second data output values is a mapping of the subset of the set of data bits to an element of a set of 2^n elements, where each non-trivial differential characteristic of each of the set of 2^n elements of the first and second output values has a probability that is less than or equal to a maximum probability;

the set of 2^n elements that provide second data output value being selected such that for each non-trivial differential characteristic having the maximum probability in the set of 2^n elements that provide the first output value, this differential characteristic has a lower probability in the set of 2^n elements that provide second data output value.

20. The cryptographic encoder of claim 18, wherein

the subset of the set of data bits consists of *n* data bits and

each of the first and second data output values is a mapping of the subset of the set of data bits to an element of a set of 2^n elements, where each non-trivial differential characteristic of each of the set of 2^n elements of the first and second output values has a probability that is at least a minimum probability and at most a maximum probability;

the set of 2^n elements that provide second data output value being selected such that for each non-trivial linear characteristic that equals the minimum or maximum probability in the set of 2^n elements that provide the first output value, this linear characteristic has a probability closer to ½ in the set of 2^n elements that provide second data output value.

EVIDENCE APPENDIX

No evidence has been submitted that is relied upon by the appellant in this appeal.

RELATED PROCEEDINGS APPENDIX

Appellant is not aware of any co-pending appeal or interference which will directly affect or be directly affected by or have any bearing on the Board's decision in the pending appeal.